

WHAT IS CLAIMED IS:

1. A method of authentication, comprising the steps of:
  - a) sending first information from a contents-information receiver apparatus to a contents-information sender apparatus, the first information including a combination of certificate information and second information for the contents-information receiver apparatus, the first information further including a signal of a signature for the combination of the certificate information and the second information;
  - b) in the contents-information sender apparatus, determining whether the combination of the certificate information and the second information in the first information is correct or wrong in response to the signal of the signature in the first information;
  - c) in the contents-information sender apparatus, extracting the second information from the first information and storing the extracted second information;
  - d) sending the second information for the contents-information receiver apparatus from the contents-information receiver apparatus to the contents-information sender apparatus; and
  - e) in the contents-information sender apparatus, collating the second information sent by the step d) with the second information stored by the step c).
2. A method as recited in claim 1, wherein the certificate

information contains information of a reliability of the contents-information receiver apparatus.

3. A contents-information sender apparatus comprising:
  - 5 first means for receiving first information from a contents-information receiver apparatus, the first information including a combination of certificate information and second information for the contents-information receiver apparatus, the first information further including a signal of a signature for the combination of the certificate information and the second information;
  - 10 second means for determining whether the combination of the certificate information and the second information in the first information received by the first means is correct or wrong in response to the signal of the signature in the first information;
  - 15 third means for extracting the second information from the first information received by the first means and storing the extracted second information;
  - 20 fourth means for receiving the second information for the contents-information receiver apparatus from the contents-information receiver apparatus; and
  - 25 fifth means for collating the second information received by the fourth means with the second information stored by the third means.
- 25 4. A contents-information sender apparatus as recited in claim 3, wherein the certificate information contains information of a

PCT/GB2008/050253

reliability of the contents-information receiver apparatus.

5. A contents-information receiver apparatus comprising:  
first means for sending first information to a contents-information sender apparatus, the first information including a combination of certificate information and second information for the contents-information receiver apparatus, the first information further including a signal of a signature for the combination of the certificate information and the second information; and  
10 second means for sending the second information for the contents-information receiver apparatus to the contents-information sender apparatus.
6. A contents-information receiver apparatus as recited in claim  
15 5, wherein the certificate information contains information of a reliability of the contents-information receiver apparatus.
7. An authentication system including a contents-information sender apparatus and a contents-information receiver apparatus, the  
20 authentication system comprising:  
first means for sending first information from the contents-information receiver apparatus to the contents-information sender apparatus, the first information including a combination of certificate information and second information for the contents-information receiver apparatus, the first information further including a signal of a signature for the combination of the  
25 information receiver apparatus, the first information further including a signal of a signature for the combination of the

certificate information and the second information;

second means provided in the contents-information sender apparatus for determining whether the combination of the certificate information and the second information in the first

5 information sent by the first means is correct or wrong in response to the signal of the signature in the first information;

third means provided in the contents-information sender apparatus for extracting the second information from the first information sent by the first means and storing the extracted

## 10 second information;

fourth means for sending the second information for the contents-information receiver apparatus from the contents-information receiver apparatus to the contents-information sender apparatus; and

15 fifth means provided in the the contents-information sender apparatus for collating the second information sent by the fourth means with the second information stored by the third means.

8. An authentication system as recited in claim 7, wherein the

20 certificate information contains information of a reliability of the  
contents-information receiver apparatus.

9. A method as recited in claim 1, wherein the certificate

information contains a signal of a public key being a mate to a secret

25 key for generating the signal of the signature from the combination  
of the certificate information and the second information.

10. A method as recited in claim 1, wherein the certificate information contains information related to a copyright on contents.

5 11. A method as recited in claim 1, wherein the certificate information contains public information given only to licensees.

10 12. A method as recited in claim 1, wherein the certificate information contains a signal of a public key peculiar to the contents-information receiver apparatus.

15 13. A method as recited in claim 1, wherein the certificate information is given to the contents-information receiver apparatus by a management organ.

20 14. A method as recited in claim 1, further comprising the step of, after the step e), exchanging a signal of a first key and a signal of a second key between the contents-information sender apparatus and the contents-information receiver apparatus.

25 15. A contents-information sender apparatus as recited in claim 3, wherein the certificate information contains a signal of a public key being a mate to a secret key for generating the signal of the signature from the combination of the certificate information and the second information.

16. A contents-information sender apparatus as recited in claim 3, wherein the certificate information contains information related to a copyright on contents.

5 17. A contents-information sender apparatus as recited in claim 3, wherein the certificate information contains public information given only to licensees.

10 18. A contents-information sender apparatus as recited in claim 3, wherein the certificate information contains a signal of a public key peculiar to the contents-information receiver apparatus.

15 19. A contents-information sender apparatus as recited in claim 3, wherein the certificate information is given to the contents-information receiver apparatus by a management organ.

20 20. A contents-information sender apparatus as recited in claim 3, further comprising sixth means for, after the collating by the fifth means, exchanging a signal of a first key and a signal of a second key with the contents-information receiver apparatus.

25 21. A contents-information receiver apparatus as recited in claim 5, wherein the certificate information contains a signal of a public key being a mate to a secret key for generating the signal of the signature from the combination of the certificate information and the second information.

22. A contents-information receiver apparatus as recited in claim 5, wherein the certificate information contains information related to a copyright on contents.

5

23. A contents-information receiver apparatus as recited in claim 5, wherein the certificate information contains public information given only to licensees.

10 24. A contents-information receiver apparatus as recited in claim 5, wherein the certificate information contains a signal of a public key peculiar to the contents-information receiver apparatus.

15 25. A contents-information receiver apparatus as recited in claim 5, wherein the certificate information is given to the contents-information receiver apparatus by a management organ.

20 26. A contents-information receiver apparatus as recited in claim 5, further comprising third means for exchanging a signal of a first key and a signal of a second key with the contents-information sender apparatus after second-information collation is done by the contents-information sender apparatus.

25 27. An authentication system as recited in claim 7, wherein the certificate information contains a signal of a public key being a mate to a secret key for generating the signal of the signature from the

combination of the certificate information and the second information.

28. An authentication system as recited in claim 7, wherein the  
5 certificate information contains information related to a copyright  
on contents.

29. An authentication system as recited in claim 7, wherein the  
certificate information contains public information given only to  
10 licensees.

30. An authentication system as recited in claim 7, wherein the  
certificate information contains a signal of a public key peculiar to  
the contents-information receiver apparatus.

15 31. An authentication system as recited in claim 7, wherein the  
certificate information is given to the contents-information receiver  
apparatus by a management organ.

20 32. An authentication system as recited in claim 7, further  
comprising sixth means for, after the collating by the fifth means,  
exchanging a signal of a first key and a signal of a second key  
between the contents-information sender apparatus and the  
contents-information receiver apparatus.